JM:JPN
F.#2008R00474

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- X

M-10-806

IN THE MATTER OF THE APPLICATION FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS:

THE THIRD FLOOR APARTMENT OF AN UNATTACHED THREE-STORY RESIDENCE WITH WHITE ALUMINUM SIDING, LOCATED AT 1053 57th STREET, BROOKLYN, NY 11219 (SUBJECT PREMISES).

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

(T. 18, U.S.C., § 1341)

- X

EASTERN DISTRICT OF NEW YORK, SS:

MARIA ALBRIGHT, being duly sworn, deposes and says that she is a United States Postal Inspector with the United States Postal Inspection Service ("USPIS"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there will be located at the premises known and described as THE THIRD FLOOR APARTMENT OF AN UNATTACHED THREE-STORY RESIDENCE WITH WHITE ALUMINUM SIDING, LOCATED AT 1053 57TH STREET, BROOKLYN, NY 11219 ("SUBJECT PREMISES") items, including a computer, that contain electronically stored information and data, and other documents, communications and electronic data and information relating to fraudulent rebate claims, all of which may constitute evidence, fruits, and instrumentalities of

violations of, among other statutes, Title 18, United States Code, Section 1341.

The source of my information and the grounds for my belief are as follows:[1]

1. I have been a United States Postal Inspector with the USPIS for approximately six years. I am familiar with the facts and circumstances of this matter from my personal participation in this investigation, a review of case files and reports, and conversations with other law enforcement officers and agents, investigators and individuals. Except where otherwise noted, all conversations described in this Affidavit are set forth in part and in substance only.

2. The statements contained in this affidavit are based in part upon my personal participation in the investigation and in part upon my conversations with other law enforcement agents.

3. During my employment with USPIS, I have participated in numerous mail fraud investigations in which I have conducted physical and wire surveillance, executed search warrants, and reviewed and analyzed documentary evidence.

---

[1] Because the sole purpose of this affidavit is to establish probable cause to search, I have not set forth a description of all the facts and circumstances of which I am aware.

I. Facts Supporting Probable Cause

4. On or about June 29, 2010, I and other federal agents arrested Seth Lowenstein ("LOWENSTEIN"), also known as "Chaim Lowenstein," pursuant to an arrest warrant issued by the United States District Court for the Eastern District of New York. We effected the arrest near LOWENSTEIN's residence, which is located at the SUBJECT PREMISES. A true and accurate photograph of the three story residence located at 1053 57th Street, Brooklyn, New York 11219 is attached as Attachment A. A true and accurate copy of the affidavit submitted in support of the arrest warrant (the "Arrest Warrant Affidavit") is attached as Attachment B, and is incorporated by reference for the purposes of this Affidavit. The Arrest Warrant Affidavit alleges that LOWENSTEIN engaged in violations of the federal mail fraud statute, Title 18, United States Code, Section 1341.

5. The Arrest Warrant Affidavit alleges, among other things, that in or around 2005, LOWENSTEIN submitted fraudulent rebate claims to 3Com, Inc. ("3Com"), a manufacturer of electronics and office products. During the time period relevant to the scheme, 3Com paid rebates to sales representatives of resellers who sold 3Com electronics products to retail customers. The term "reseller" refers to companies or entities that purchased products from 3Com and, in turn, sold those products to retail customers.

6. In connection with the scheme alleged in the Arrest Warrant Affidavit, LOWENSTEIN submitted false information to 3Com about 3Com products that he purportedly sold to retail customers. That information was submitted to 3Com electronically over the Internet via a 3Com website. The information that LOWENSTEIN submitted was false and the purported sales were fictitious.

7. The Arrest Warrant Affidavit further alleges that LOWENSTEIN submitted fraudulent invoices to 3Com through the mail in an effort to further his scheme. Those invoices purportedly contained information reflecting sales by LOWENSTEIN to retail customers. The invoices identified in the Arrest Warrant Affidavit were mailed from Brooklyn, New York. 3Com paid rebates to LOWENSTEIN in connection with the fraudulent rebate claims that he submitted.

8. On or around June 29, 2010, shortly after LOWENSTEIN's arrest, I and another federal agent interviewed LOWENSTEIN. Prior to conducting the interview, I provided LOWENSTEIN with his Miranda warnings, which LOWENSTEIN acknowledged and understood.

9. During the interview, among other things, LOWENSTEIN read the Arrest Warrant Affidavit and indicated that the Arrest Warrant Affidavit was accurate, and that he did not disagree with the allegations contained in the document.

10. During the interview, LOWENSTEIN stated that he began submitting fraudulent rebate claims to 3Com in 1998, and that he continued to submit fraudulent rebate claims to 3Com and other corporations through at least 2008.

11. During the interview, LOWENSTEIN stated that he submitted fraudulent rebate claims to multiple electronics corporations, including 3Com, Hewlett Packard, IBM, Staples, Lexmark, and Philips. In connection with many of the rebate claims, LOWENSTEIN submitted false invoices to the corporations. LOWENSTEIN created false invoices and submitted those invoices the 3Com and other corporations to create the impression that LOWENSTEIN actually sold products to particular retail customers.

12. LOWENSTEIN stated that he used a computer located at the SUBJECT PROPERTY to create fraudulent invoices that he submitted to 3Com and other corporations during the course of the scheme. LOWENSTEIN confirmed that he lives alone at the SUBJECT PREMISES and that there are no other apartments located on third floor of 1053 57th Street, Brooklyn, New York 11219.

13. LOWENSTEIN also stated that he used various names in connection with the fraudulent rebate scheme, and that he often submitted claims on behalf of various companies. Some of the names LOWENSTEIN used in connection with his rebate scheme included: Tuvia Kaplan, Chayim Lowenstein, Haim Lowenstein, Schmuel Chayim, Bru Leigh, C Lowenstein, SM Lowenstein, Tom Kane, Tommy Kane, and C Pliskey. The company names through which

LOWENSTEIN submitted fraudulent rebate claims included, among others: Keep on Smiling, KOS, Armorcore, Webcommerce, Webcom247, You Gotta Own Real Estate, and YGORE. LOWENSTEIN stated that he often received rebate checks from 3Com and other corporations and deposited those checks into bank accounts that he controlled. Some of those bank accounts were not maintained in LOWENSTEIN's name.

14. He further stated that he opened accounts with commercial mail receiving agencies or "CMRAs" in Florida, Michigan, and New York. LOWENSTEIN used the CMRAs to receive mail in connection with the rebate scheme.

15. In my experience, I am aware that CMRAs are authorized to receive mail and packages on behalf of customers. Typically, CMRAs assign each customer a specific mail box number. Additionally, CMRAs often forward mail on behalf of customers to other locations.

16. Based upon the facts set forth above, as well as my training and experience, I know that those involved in fraudulent schemes frequently maintain in their possession, for substantial periods of time, items, including computers, that contain electronically stored information and data, and other documents, communications and electronic data and information relating to the fraudulent schemes, all of which may constitute evidence, fruits, and instrumentalities of violations of, among other statutes, Title 18, United States Code, Sections 1341.

II. Search Methodology to be Employed

17. Because this Affidavit seeks a warrant to seize and search computers and computer related equipment, I set forth below the manner in which the search of these items will occur, should the requested warrant be issued.

18. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, external hard drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In

addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will likely be highly impractical to search for data at the time of its seizure. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5

million pages of data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

19. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant, to the extent applicable, will employ the following procedure:

a. Law enforcement personnel trained in seizing computer data (the "computer personnel") will seize any computers

and any associated computer equipment and storage devices and transport those items to an appropriate law enforcement laboratory for review. Any computer and any associated computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

20. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not: (a) an instrumentality of the offenses; (b) a fruit of the criminal activity; (c) contraband; (d) otherwise unlawfully possessed; or (e) evidence of the offenses specified above.

21. In searching the data, the computer personnel may examine all of the data contained in any computers and any associated computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

22. If the computer personnel determine that any computer and any associated computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to

Federal Rule of Criminal Procedure 41(b), the Government will return these items, upon request, within a reasonable period of time.

23. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques and procedures (the following is a non-exclusive list, as other search techniques and procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. scanning storage areas to discover and possibly recover recently deleted files;

d. scanning storage areas for deliberately hidden files;

e. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the

criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the items to be seized; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the items to be seized.

24. In conducting the search of any computer, electronic storage device, closed, or locked container authorized by the this Search Warrant, the government shall make reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information which are identified in the Search Warrant itself.

WHEREFORE, I respectfully request that a search warrant issue allowing United States Postal Inspectors and other federal agents, with proper assistance from other law enforcement officers, to search, gain access to, and retrieve from the SUBJECT PREMISES, the following items, whether in document form or stored on any electronic optical or computer media, located at the SUBJECT PREMISES:

a. All items and documents that refer or relate to:
IBM,
Hewlett Packard,
3Com, Inc.,
Philips,
Lexmark,
Tuvia Kaplan,

Chayim Lowenstein,
Haim Lowenstein,
Schmuel Chayim,
Bru Leigh,
C Lowenstein,
SM Lowenstein,
Tom Kane,
Tommy Kane,
C Pliskey,
Keep on Smiling,
KOS,
Armorcore,
Webcommerce,
Webcomm 247,
You Gotta Own Real Estate, and
YGORE;

b. All bank records for the period 1998 through 2008;

c. Computer hardware, meaning any and all computers and electronic devices, including computer components, diskettes, computer peripherals, monitors, plotters, encryption circuit boards, optical scanners, external hard drives, and other computer-related electronic devices;

d. Computer software, meaning any and all instructions or programs stored in the form of electronic or magnetic media which are capable of being interpreted by a computer related component. The items to be seized include operating systems, application software, utility programs, compilers, interpreters, and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, cable connections, radio or other means of transmissions;

e. All documents relating to any mail box located at a commercial mail receiving agency, including customer applications and correspondence;

f. All documents relating to any rebate claim;

g. All documents relating to the sale of any electronics or office product, including any invoice.

h. All stored e-mail, text messages, "chat," or instant messages, including any attachments to such e-mails or messages, sent by or received by the user(s) of any computer located at the SUBJECT PREMISES, whether saved or deleted, and whether contained directly in an e-mail, text message, chat, or instant message account or in a customized "folder" constituting or showing evidence and instrumentalities of mail fraud relating to fraudulent rebate claims;

i. All web-pages, internet browsing history, "cookies," and "bookmarks," including any associated links, that were created or maintained by the user(s) of any computer located at the SUBJECT PREMISES constituting or showing evidence and instrumentalities of mail fraud relating to fraudulent rebate claims, including, but not limited to, visits to websites such as 3COM, Lexmark, Staples, Philips, IBM, and Hewlett Packard;

j. All spreadsheet, database, presentation, or word-processing files created or maintained by the user(s) of any computer located at the SUBJECT PREMISES, including, but not limited to, Excel, Access, PowerPoint, Publisher, Visio, Quicken, Word, Word Perfect, WordPad and Notepad files constituting or showing evidence and instrumentalities of mail fraud relating to fraudulent rebate claims;

k. All calendar, contact, or personal planner data or files, including, but not limited to, data contained in Outlook, Lotus Notes, or Eureka, created or maintained by the user(s) of any computer located at the SUBJECT PREMISES constituting or showing evidence and instrumentalities of mail fraud relating to fraudulent rebate claims;

l. All contact information or call data relating to online voice or video communication services, including, but not limited to, Voice Over Internet Protocol (VOIP) communications on Skype or Vonage, created or maintained by the user(s) of any computer located at the SUBJECT PREMISES constituting or showing evidence and

instrumentalities of mail fraud relating to fraudulent rebate claims; and

m. All backup files for the items described above constituting or showing evidence and instrumentalities of mail fraud relating to fraudulent rebate claims.

all of which may constitute evidence, fruits, and instrumentalities of violations of, among other statutes, Title 18, United States Code, Sections 1341.

Maria Albright
U.S. Postal Inspector
U.S. Postal Inspection Service

Sworn to before me this
15 day of July, 2010

UI
E

ATTACHMENT A

JM:JPN

[redacted]-10-730

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA

-against-

SETH LOWENSTEIN,
also known as
"Chaim Lowenstein,"

Defendant.

----------X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT

(Title 18, U.S.C., §§ 1341 and 3551 et seq.)

EASTERN DISTRICT OF NEW YORK, SS:

MARIA ALBRIGHT, being duly sworn, deposes and says that she is a United States Postal Inspector with the United States Postal Inspection Service, duly appointed according to law and acting as such.

In or about and between October 2005 and December 2005, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant SETH LOWENSTEIN, also known as "Chaim Lowenstein," knowingly and intentionally devised a scheme and artifice to defraud, and obtained money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, did place and cause to be placed in a post office and authorized depository for mail matter, false documents to be sent and delivered by the United States Postal Service.

ATTACHMENT B

(Title 18, United States Code, Sections 1341 and 3551 et seq.)

The source of your deponent's information and the grounds for her belief are as follows:

1. I am a United States Postal Inspector with the United States Postal Inspection Service and have been so employed for approximately six years. I am currently assigned to the Fraud Team which investigates allegations of fraud involving the United States Postal Service. In this position, I have conducted surveillance, interviewed witnesses, reviewed extensive documents obtained through the service of subpoenas, and used other investigative techniques to secure relevant information for use in criminal prosecutions.

2. The facts set forth in this affidavit were developed as a result of an investigation conducted by me and other law enforcement officers, interviews of witnesses, conversations with other law enforcement agents and the review and analysis of documents and records relating to the investigation.[1]

[1] Because the purpose of this affidavit is limited to setting forth probable cause to arrest, I have not set forth every fact of which I am aware pertaining to this investigation. Where I relate statements, conversations, and actions of others, those statements, conversations, and actions of others are related in substance and in part, except where otherwise indicated.

BACKGROUND

A. The Rebate Program

3. During the time period of the scheme, 3Com Inc. (hereinafter referred to as "3Com") was a large manufacturer of office and electronic products and supplies, and its corporate headquarters were located in Marlborough, Massachusetts. During the time period of the scheme, 3Com operated a program (hereinafter referred to as the "3Com Rewards Program") through which it paid rebates to sales representatives of resellers of 3Com office and electronic products. 3Com used the term "reseller" to refer to companies or entities that purchased products from 3Com and, in turn, sold those products to retail customers. 3Com referred to retail customers as "end users." The 3Com Rewards Program allowed sales representatives of resellers to receive rebates for selling certain 3Com products to end users.

4. To be eligible for the 3Com Rewards Program, a sales representative had to register with 3Com and authorize 3Com to open a debit card (hereinafter referred to as the "Rebate Card") in the sales representative's name. 3Com distributed Rebate Cards to the sales representatives who registered with 3Com as part of the rebate program.

5. To submit a claim for a rebate in connection with the 3Com Rewards Program, a sales representative had to provide

information to 3Com about each rebate-eligible 3Com product that he or she sold to an end user. That information had to be submitted to 3Com electronically over the Internet via the 3Com Rewards Program website.

6. Among other things, a sales representative had to provide 3Com with the invoice number of the end user's invoice (hereinafter referred to as the "End User Invoice"). The term "End User Invoice" referred to the sale invoice provided by a reseller to an end user in connection with the end user's purchase of a 3Com product.

7. To submit a claim for a rebate, a sales representative also had to mail a copy of each End User Invoice, as well as specific information obtained from the 3Com Rewards website, to 3Com's office in Grand Rapids, Minnesota. The information obtained from the 3Com website consisted of a one page summary of the rebate claim that contained the sales representative's name as well as the End User Invoice number associated with the claim.

8. 3Com paid rebates in connection with the 3Com Rewards Program by depositing funds directly into the account associated with the sales representative's Rebate Card.

THE FRAUDULENT SCHEME

9. During the time period of the scheme, the defendant SETH LOWENSTEIN registered with 3Com as a purported

sales representative in connection with the 3Com Rewards Program. Instead of using his own name, LOWENSTEIN registered under the name of "Chaim Lowenstein." Using the name "Chaim Lowenstein," LOWENSTEIN submitted rebate requests for fictitious or nonexistent sales of 3Com products. In connection with this scheme, LOWENSTEIN mailed fraudulent End User Invoices from Brooklyn, New York to 3Com's office in Grand Rapids, Minnesota.

10. For example, on or about November 23, 2005, LOWENSTEIN mailed two End User Invoices (hereinafter referred to as the "November Invoices") to the 3Com's Grand Rapids, Minnesota office via a Priority Mail envelope (hereinafter referred to as the "November 2005 Mailing"). The return address on the November 2005 Mailing listed "WebCom247" and the address of 1053 57 Street, Ste. 3, Brooklyn, NY 11219 (hereinafter referred to as the "1053 57 Street Address").

11. The November Invoices were purportedly submitted by "Chaim Lowenstein," who, according to 3Com's records, had registered in connection with the 3Com Rewards Program as a sales representative of "WebCom247," a purported 3Com reseller.

12. The letterhead on the November Invoices listed WebCom247 and the 1053 57 Street Address.

13. The November Invoices indicated that WebCom247 had sold 3Com electronic products, valued at over $30,000, to Esker,

Inc. and listed Esker, Inc.'s address as 100 East 7th Avenue, Stillwater, Oklahoma.

14. One of the November Invoices indicated that a portion of the 3Com computer products purportedly sold to Esker, Inc. had been shipped by WebCom247 to Esker Inc.'s office in Connecticut.

15. On or about December 14, 2005, 3Com paid "Chaim Lowenstein" a rebate in the amount of $1,100 in connection with the November Invoices. 3Com paid the rebate by crediting the account associated with the Rebate Card issued to "Chaim Lowenstein."

16. The November Invoices were fraudulent. An employee of Esker Inc. has informed me, in sum and substance, that WebCom247 is not a vendor of Esker, Inc. and is not listed in Esker, Inc.'s accounts payable system. Moreover, Esker, Inc. has no record of ever doing business with any vendor located in the 11219 zip code, and it has no record of any payment made to "WebCom247."

17. The Esker, Inc. employee also informed me, in sum and substance, that the computer products listed on the November Invoices are not products that Esker, Inc. would have purchased or used in the course of its business. The employee also informed me that Esker, Inc. has never had an office in Connecticut.

18. 3Com records indicated that, during the time period of the scheme, the defendant SETH LOWENSTEIN, using the name "Chaim Lowenstein," submitted multiple rebate claims to 3Com in connection with the 3Com Rewards Program. I have communicated with the end users listed on End User Invoices submitted in connection with those claims, and as a result of those communications, I have determined that the purported sales referenced in the rebate claims submitted by "Chaim Lowenstein" also were ficticious.

19. The estimated total loss associated with LOWENSTEIN's conduct involving the 3Com Rewards Program is $24,240. Additionally, records obtained from 3Com indicate that the defendant SETH LOWENSTEIN engaged in additional fraudulent conduct in connection with another 3Com rebate program. Our investigation of that conduct is ongoing, and the estimated loss associated with that conduct substantially exceeds the estimated loss associated with the 3Com Rewards Program.

A. **The Defendant Used the Alias "Chaim Lowenstein"**

20. On or around November 13, 2008, I conducted surveillance at the 1053 57 Street Address. During my surveillance, I observed a white male exit the 1053 57 Street Address. The white male then got into the driver's seat of a white, four-door Dodge automobile that was parked nearby, and drove away. I subsequently determined that the white Dodge

automobile, which had a Florida license plate, was registered to the defendant SETH LOWENSTEIN, and I determined, based upon my review of known photographs of LOWENSTEIN, that the man that I observed was LOWENSTEIN.

21. Records obtained from the Department of Motor Vehicles (hereinafter referred to as the "DMV") for the State of Florida indicated that the defendant SETH LOWENSTEIN resided at 10920 Baymeadows Road, #27,154, Jacksonville, FL 32256-4570.

22. The residential address listed for the defendant SETH LOWENSTEIN in the DMV records is actually a mail drop operated by PakMail, a commercial mail receiving agency or "CMRA."

23. As a CMRA, PakMail is authorized to receive mail and packages on behalf of customers. PakMail assigns each customer a specific mail box number. PakMail records indicated that the defendant SETH LOWENSTEIN became a customer of PakMail in or about August 2007, and that PakMail assigned LOWENSTEIN mail box number 154.

24. Records obtained from PakMail indicated that the defendant SETH LOWENSTEIN and "Chaim Lowenstein" are the same person. In fact, the application submitted by LOWENSTEIN to PakMail to authorize PakMail to receive mail on LOWENSTEIN's behalf (hereinafter referred to as the "PakMail Application")

identifies LOWENSTEIN as "Chaim Lowenstein a/k/a Seth Lowenstein."

25. The PakMail Application also indicated that LOWENSTEIN submitted two forms of identification to PakMail in connection with his application. Specifically, LOWENSTEIN provided PakMail with a Florida driver's license in LOWENSTEIN's name and a business card in the name of "Chaim Lowenstein." The business card stated that "Chaim Lowenstein" was the CTO and COO of "WebCom247." The business card also contained a photograph of "Chaim Lowenstein." That photograph appears to be a photograph of LOWENSTEIN. PakMail retained copies of the two forms of identification provided by LOWENSTEIN.

26. A review of the defendant SETH LOWENSTEIN's criminal history reveals that he was convicted in 1993 in Nassau County, New York, First District Court, of Possession of a Forged Instrument in the Second Degree and Grand Larceny in the Third Degree. In connection with those convictions, he was sentenced to thirty days in prison and five years probation.

Wherefore, it is respectfully requested that a warrant be issued for defendant SETH LOWENSTEIN, also known as "Chaim Lowenstein," so that he may be dealt with according to law.

MARIA ALBRIGHT
United States Postal Inspector
United States Postal Inspection Service

Sworn to before me this
25th day of June 2010

E